HOUSE OF REPRESENTATIVES

BILLs

Cybercrime Legislation Amendment Bill 2011

Second Reading

SPEECH

Wednesday, 22 June 2011

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES
Mr McCLELLAND (Barton—Attorney-General) (09:05): I move:

That this bill be now read a second time.

The Cybercrime Legislation Amendment Bill 2011 makes amendments to facilitate Australia’s accession to the Council of Europe Convention on Cybercrime.

The convention is the only binding international treaty on cybercrime.

The government announced its intention to accede to the convention in April 2010. To date, over 40 nations have either signed or become a party to the convention, including the United States, United Kingdom, Canada, Japan, South Africa and others.

Cybercrime poses a significant challenge for our law enforcement and criminal justice system. The global and interconnected nature of the internet makes it easy for malicious actors to operate from abroad, especially from those countries where regulations and enforcement arrangements are weak. For this reason, it is critical that laws designed to combat cyberthreats are harmonised, or at least compatible to allow for international cooperation between law enforcement agencies.

The convention serves as a guide for nations developing comprehensive national legislation on cybercrime and also establishes procedures to make investigations more efficient and provides systems to facilitate international cooperation, including:

- empowering authorities to request the preservation of specific communications;
- helping authorities from one country to collect data in another country;
- establishing a 24/7 network to provide immediate help to investigators; and
- facilitating the exchange of information.

The convention requires parties to criminalise certain types of conduct committed via the internet and other computer networks and ensure domestic agencies can access and share information to facilitate international investigations.

As such, the convention will help Australian agencies to better prevent, detect and prosecute cyberintrusions and criminal activity conducted over the internet.

Australian law already complies with a majority of the obligations of the convention. In particular, jurisdictions in Australia have created relevant offences and have provided agencies with many of the powers and procedures required by the convention.

However, accession to the convention will require amendments to the Telecommunications (Interception and Access) Act 1979, the Mutual Assistance in Criminal Matters Act 1987, the Criminal Code Act 1995 and the Telecommunications Act 1997 to enhance Australia’s ability to effectively combat cybercrime.

**Preservation of stored communications**

In terms of an overview of the act, schedule 1 implements requirements of the convention to establish powers for agencies to obtain the preservation of stored communications for up to 90 days, particularly where there are grounds to believe that the data is vulnerable to loss or to modification.
The purpose of the preservation period is to maintain the integrity of the data for a period of time to enable agencies to seek its disclosure through a relevant warrant.

These amendments are necessary as carriers’ business practices often include the deletion of communications before agencies have the opportunity to exercise a warrant for their access, in the case of one carrier that is within 24 hours of a message’s creation. It also, however, on the other side of the coin, formalises cooperative and voluntary arrangements that already exist with some carriers who will hold communication records pending formal receipt of a warrant.

Accordingly, the bill amends the Telecommunications (Interception and Access) Act so that an agency can formally require a carrier to preserve stored communications by reference to an individual or telecommunications service. This approach enables the preservation of computer data, but also SMS messages, emails and other communications stored by the carrier while ensuring the Telecommunications (Interception and Access) Act remains technologically neutral.

The bill will also enable designated interception agencies to require carriers to preserve ongoing communications in respect to an individual or service for up to 30 days. Again, these communications can only be accessed by a designated interception agency upon the grant of a valid warrant.

The bill will enable the Australian Federal Police to require the preservation of communications on behalf of a foreign law enforcement agency. Once again, however, the content of those preserved communications can only be accessed following authorisation of a stored communications warrant under a formal mutual assistance request for a serious foreign contravention. Such a serious contravention is an offence carrying a penalty of either three years imprisonment or a fine of approximately $99,000.

There are a number of important protections in the bill and these include the fact that:

Agencies can only access preserved communications from a carrier with a relevant warrant.

Preservation is only available to investigate a ‘serious contravention’ (defined as an offence carrying three years’ imprisonment, a $19,800 fine for individuals, and a $99,000 for nonindividuals) or for obtaining intelligence relating to security which is defined under the ASIO Act as relating to espionage, terrorism, foreign interference and border integrity.

In each case a number of tests must also be satisfied. These include balancing privacy considerations and determining that there are reasonable grounds to suspect that the carrier holds the relevant communications and also that the information obtained would be likely to assist the investigation.

Also included in the protections are the fact that domestic notices are revoked automatically after 90 days. They must also be revoked by the agency if before that point in time the agency is no longer satisfied that grounds exist for issuing the notice.

The other protections include notices with respect to the preservation of ongoing communications which are only available for up to 30 days in the case of ongoing communications.

Agencies will be required to report on the number of preservation notices issued and keep copies of those notices.

Finally, the use of preservation powers by agencies will be subject to the oversight of the Commonwealth Ombudsmen in respect to policing agencies and the Inspector-General of Intelligence and Security (IGIS) in respect to the actions of ASIO.

International cooperation

In terms of international cooperation, schedule 2 of the bill amends the Telecommunications (Interception and Access) Act 1979 and the Mutual Assistance in Criminal Matters Act 1987 to allow the Australian Federal Police to assist foreign partners by accessing communications data on a police-to-police basis. Communications data relates to information about a communication, rather than the content of the communication itself. This is often important information which can reveal a target has Australian accounts, has been involved with known Australian suspects or has connections or associations with known criminal groups. The bill will also enable Australia to provide non-content data on an ongoing basis to a foreign country, following a formal mutual
assistance request. Particular safeguards with respect to providing information pursuant to a mutual assistance
request will also apply. These tools will further assist in the investigation of international cybercrime.

In order to ensure full compliance with article 15 of the convention, which deals with the protection of civil
liberties, the bill also introduces a new requirement in the Telecommunications (Interception) Act in respect of
the protection of privacy. This will require agencies to specifically consider the privacy of affected parties before
authorising the disclosure of telecommunications data.

The requirement to consider privacy will apply to any authorisation for any domestic or foreign purpose. Privacy
in this context, is interpreted more broadly than in the Privacy Act 1988, and will include consideration of the
amount of information that the authorisation will make available to the agency, the relevance of the accessed
information to the investigation in question, as well as how a third party’s privacy may be impacted by the
information.

The reforms contained in schedule 2 were released for public comment by the government in January 2011 in
respect of the Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Bill.

Amendments to the Criminal Code

Computer crimes in Australia are set out in Commonwealth as well as state and territory law.

Commonwealth offences are currently limited to circumstances in which a carriage service has been used or
Commonwealth computers or data are involved in the commission of an offence. For situations not covered by
Commonwealth laws, state and territory offences are used by law enforcement agencies.

In order to ensure full compliance with convention requirements, the Criminal Code will be amended to remove
the current limitations on Commonwealth computer offences. The amended powers will be supported by the
external affairs power, Australia implementing this legislation as part of its compliance with that international
treaty obligation.

In the event of any inconsistency between Commonwealth and state or territory laws, the savings provisions
contained in the Criminal Code will ensure the validity of those state and territory laws.

Consultation

In April 2010, the then Minister for Foreign Affairs and I jointly announced Australia’s intention to accede to
the convention. On 17 February 2011, the Attorney-General’s Department released a public discussion paper in
relation to Australia’s proposed accession.

Submissions were received from representatives of the telecommunications industry, state governments, the
Office of the Information Commissioner as well as from privacy and civil liberties groups.

The majority of submissions supported accession.

After the tabling of the national interest analysis by the Minister for Foreign Affairs on 1 March 2011, the Joint
Standing Committee on Treaties considered Australia’s proposed accession. JSCOT tabled its report supporting
Australia’s accession to the convention on 11 May 2011. The committee agreed that cybercrime is a growing
threat at a time when computer based networks are the most vital means of communicating and doing business.

Conclusion

The increasing cybercrime threat means that no nation alone can effectively overcome this problem and that
international cooperation is essential.

Australia must have appropriate arrangements domestically and internationally to be in the best possible position
to fight cybercrime and to do it in cooperation with international partners.

This bill will facilitate Australia’s accession to the cybercrime convention and improve our ability to cooperate
internationally and domestically in combating cybercrime. I commend the bill to the House.
Debate adjourned.